CLAIMS:

1. A method for secure communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by a relatively insecure intermediate network, the method including the steps of:

selectively routing a communication from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of one or more network elements triggerable to selectively route said communication; and

encrypting said selectively routed communication by means of an encryption engine before it traverses said intermediate network,

wherein said one or more network elements and said encryption engine are located substantially within said first secure network.

2. A method as in claim 1, wherein said one or more network elements comprises switch means provided with control means and storage means.

3. A method as in claim 2, wherein said storage means is operable to store routing information.

4. A method as in claim 2 or 3, wherein said storage means is operable to store security information.

5. A method as in claim 2, 3 or 4, wherein said storage means is operable to store security information including one or more of the following: encryption information; decryption information; security key information; and electronic cash information.

6. A method as in any of claims 3 to 5, wherein said switch means is operable to selectively route a predetermined

communication according to routing information held in the storage means.

7. A method as in any of claims 4 to 6, wherein said encryption engine is operable to encrypt said predetermined communication according to security information held in said storage means.

8. A method as in claim 6 or 7, comprising the step of identifying said predetermined communication by means of one or more of the following: originating subscriber characteristics; destination subscriber characteristics; destination subscriber characteristics; payload characteristics; and network service characteristics.

9. A method as in claim 8, wherein said predetermined communication is identified by means of the originating and/or destination address.

10. A method as in claim 8, wherein said predetermined communication is identified by means of originating and/or destination identification numbers.

11. A method as in any of claims 4 to 10, wherein said storage means is operable to store security information, said security information being distributed from a first node to one or more target nodes responsive to a predetermined trigger.

12. A method as in any of claims 3 to 11, wherein the stored routing information includes subscriber routing preferences.

13. A method as in any of claims 4 to 12, wherein the security information includes subscriber security preferences.

14. A method as in any of claims 4 to 13, wherein the security information includes encryption/decryption

information defining a preferred algorithm or key for use with predetermined types of communication.

15. A method as in any of claims 2 to 14, wherein information stored in the storage means is arranged to identify one or more groups of users whose communications are to be routed and encrypted according to common preferences.

16. A method as in any of claims 2 to 15, wherein a service management access point is provided for accessing and changing information held in the storage means.

17. A method as in any of claims 11 to 16, wherein said security information comprises decryption information, the distribution of said decryption information being triggered according to a predetermined schedule.

18. A method as in any of claims 11 to 17, wherein said security information is distributed to a node within one or more of the first and second secure networks.

19. A method as in any of claims 11 to 18, wherein said security information is distributed to the end terminal for the communication in question.

20. A method as in any of claims 11 to 19, wherein the one or more network elements distributes security information from a location substantially within the first secure network.

21. A method as in any of claims 11 to 20, wherein one or more network elements distributes security information from a location substantially within the second secure network.

22. A method as in claim 21, wherein security information is transferred to the one or more network elements located in the second secure network by means of a secure communication route operated by trusted network operators.

23. A method as in claim 21, wherein security information is transferred to the one or more network elements located in the second secure network by means of a secure communication route over a relatively insecure intermediate network.

24. A method according to any preceding claim, provided to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network.

25. A method for the distribution of security information between a first node and one or more second nodes, including the step of providing one or more network elements operable to store security information and triggerable to distribute the security information from said first node to one or more target nodes.

26. A method for the distribution of security information between a first node in a first secure network and one or more nodes in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to one or more of said second nodes via said relatively insecure network are encrypted, including the step of providing one or more network elements operable to store security information and triggerable to distribute security information in a secure manner from said first node to one or more target nodes in said second secure network.

27. A secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by a relatively insecure intermediate network, the secure network arrangement including:

one or more network elements triggerable to selectively route a communication from the first end terminal to the

second end terminal over said relatively insecure intermediate network; and

an encryption engine for encrypting said selectively routed communication before it traverses said intermediate network,

wherein said one or more network elements and said encryption engine are located substantially within said first secure network.

28. A secure network arrangement according to claim 27, wherein said one or more network elements comprise a switch means provided with a control means and a storage means for storing routing and encryption/decryption information.

29. A secure network arrangement according to claim 28, wherein the switch means is operable selectively route a predetermined type of communication according to routing information held in the storage means and the encryption engine is operable encrypt said selectively routed communication according to encryption information held in said storage means.

30. A secure network arrangement according to claim 29, wherein said predetermined types of communication are identified by means of one or more of the following: originating subscriber characteristics; destination subscriber characteristics; payload characteristics or network service characteristics.

31. A secure network arrangement according to claim 30, wherein said predetermined types of communication are identified by means of the originating or destination address.

32. A secure network arrangement according to claim 31, wherein said predetermined types of communication are identified by means of originating identification or destination numbers.

33. A secure network arrangement according to claim 31, wherein the routing information and encryption/decryption information specifies operations according to subscriber preferences.

34. A secure network arrangement according to claim 33, wherein the encryption/decryption information defines a preferred algorithm or key for use with said predetermined types of communication.

35. A secure network arrangement according to claim 34, wherein the information held in the storage means identifies one or more groups of users whose communications are to be routed and encrypted according to common preferences.

36. A secure network arrangement according to any preceding claim, comprising a service management access point for accessing and changing information held in the storage means.

37. A secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by one or more intermediate networks at least one communication route through which constitutes a relatively insecure communication route from the first end terminal to the second end terminal, the secure network arrangement including one or more network elements triggerable to selectively route a communication from the first end terminal to the second end terminal over said relatively insecure intermediate network; and

an encryption engine for encrypting said selectively routed communication before it traverses said interemediate network, wherein said one or more network elements and said encryption engine are located substantially within said first secure network.

38. A secure network arrangement according to any preceding

claim, including decryption means located substantially within the second secure network.

39. A secure network arrangement according to claim 38, wherein said decryption means are provided at the second end terminal.

40. A secure network arrangement according to claim 38, wherein said decryption means are provided at a node other than the second end terminal.

41. A method for the distribution of security information between a first node in a first secure network and one or more nodes in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to one or more of said second nodes via said relatively insecure network are encrypted, the method comprising providing one or more network elements operable to store security information and being triggerable to distribute said security information in a secure manner from said first node to one or more target nodes in said second secure network.

42. A network arrangement for the distribution of security information between a first node in a first secure network and one or more nodes in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to one or more of said second nodes via said relatively insecure network are encrypted, the network arrangement comprising one or more network elements operable to store security information and triggerable to distribute said security information in a secure manner from said first node to one or more target nodes in said second secure network.

43. A network arrangement according to claim 42, which is operable to distribute security information including one or

more of encryption algorithms; decryption algorithms; security keys; and electronic cash bit strings.

44. A network arrangement according to claim 42 or 43, wherein the one or more network elements comprise switch means provided with control means, and storage means for storing said encryption/decryption information.

45. A network arrangement according to claim 42, wherein said switch means is operable to selectively distribute security information in response to a predetermined type of communication.

46. A network arrangement according to claim 45, wherein said predetermined type of communication is identified by means of originating subscriber characteristics, destination subscriber characteristics, payload characteristics or network service characteristics.

47. A network arrangement according to claim 42, 43 or 44, wherein said distribution is triggered according to a predetermined schedule.

48. A network arrangement according to any of claims 42 to 47, comprising a service management access point.

49. A network arrangement according to any of claims 42 to 48, wherein the security information is distributed to a node within one or more of the first secure network and second secure network, rather than the destination end terminal for the communication in question.

50. A network arrangement according to any of claims 42 to 49, wherein the security information is distributed to the end terminal for the communication in question.

51. A network arrangement according to any of claims 42 to

50, wherein the one or more network elements distributes security information from a location substantially within the first secure network.

52. A network arrangement according to any of claims 42 to 51, wherein the one or more network elements distributes the security information from a location substantially within one of the first or second networks.

53. A network arrangement according to claim 52, wherein security information is transferred to the one or more network elements located in the second secure network by means of a secure communication route operated by trusted network operators.

54. A network arrangement according to claim 53, wherein security information is transferred to the one or more network elements located in the second secure network by means of a secure communication route over a relatively insecure intermediate network.

55. A network arrangement for the distribution of security information between a first node and one or more second nodes, including one or more network elements operable to store security information and triggerable to distribute the security information from said first node to one or more of said second nodes.

56. A network arrangement for the distribution of security information between a node in a first secure network and one or more nodes in a second secure network, said first and second networks being separated by a relatively insecure intermediate network, including:

in at least one of said first and second secure networks one or more network elements operable to store security information and triggerable to distribute security information to one or more target nodes in said second secure network; and

an encryption engine for encrypting a communication before it traverses said intermediate network.

57. A method for the distribution of security information between a first node and one or more second nodes, including the step of providing one or more network elements operable to store security information and triggerable to distribute the security information from said first node to one or more target nodes.

58. A method for the distribution of security information between a first node in a first secure network and one or more nodes in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to one or more of said second nodes via said relatively insecure network are encrypted, including the step of providing one or more network elements operable to store security information and triggerable to distribute security information in a secure manner from said first node to one or more target nodes in said second secure network.

59. A method according to claim 16 or 17, provided to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network.